What is claimed is:

1. A method of digital rights management (DRM), comprising the steps of:

receiving content at a client computer, wherein the content is encrypted with an encryption key;

the client computer requesting the encryption key from a server using a digital certificate, wherein the server is remote from the client computer;

the server receiving the request; and

determining if the digital certificate is valid.

2. The method of claim 1, wherein if the digital certificate is valid the method further comprises the steps of:

transmitting the encryption key to the client computer; and

the client computer decrypting the content with the encryption key.

3. The method of claim 2, further comprising the steps of:

encrypting the encryption key, wherein:

the transmitting step transmits the encrypted encryption key to the client computer; and

the client computer decrypting the encrypted encryption key.

4. The method of claim 3, further comprising the step of:

determining a hardware profile of the client computer, wherein:

the encrypting step encrypts the encryption key with the hardware profile of the client computer.

5. The method of claim 4, wherein:

the hardware profile of the client computer is stored and linked with a copy of the digital certificate on the server; and

the determining step retrieves the hardware profile that is linked with the copy of the digital certificate.

6. The method of claim 2, wherein encryption key is only stored in volatile memory of the client computer.

7. The method of claim 1, wherein:

a first hardware profile of the client computer is stored and linked with a copy of the digital certificate on the server;

the requesting step includes transmitting a second hardware profile of the client computer to the server; and

the determining step determines whether the second hardware profile is the same as the first hardware profile.

8. The method of claim 7, wherein the digital certificate includes a public key of a public key infrastructure (PKI) key pair and the method further comprises the step of:

encrypting the second hardware profile of the client computer with a random session key; and

encrypting the random session key with the public key of the PKI key pair.

9. The method of claim 8, wherein:

a copy of the digital certificate including a private key of the PKI key pair is stored on the server; and

the determining step includes decrypting the random session key with the private key of the PKI key pair.

10. The method of claim 1, wherein:

the digital certificate includes a certificate serial number;

a copy of the digital certificate that includes the certificate serial number is stored on the server;

the requesting step includes transmitting the certificate serial number to the server; and

the determining step includes retrieving the copy of the digital certificate using the certificate serial number.

11. The method of claim 1, wherein the receiving step receives content from a website server.

12. The method of claim 1, wherein the server is a first server and the receiving step receives content from a second server co-located with the first server.

13. A system for digital rights management comprising:

a client computer, wherein the client computer includes software comprising instructions for:

receiving content, wherein the content is encrypted with an encryption key; and

requesting the encryption key from a digital rights management (DRM) server using a digital certificate, wherein the server is remote from the client computer; and

the server, wherein the server includes software comprising instructions for:

receiving the request; and

determining if the digital certificate is valid.

14. The system of claim 13, wherein the server software further comprises instructions for:

if the digital certificate is valid, transmitting the encryption key to the client computer

15. The system of claim 14, wherein the client computer software further comprises instructions for:

decrypting the content with the encryption key.

16. The system of claim 13, wherein the server software further comprises instructions for:

encrypting the encryption key, wherein the transmitting instruction transmits the encrypted encryption key to the client computer.

17. The system of claim 16, wherein the server software further comprises instructions for:

determining a hardware profile of the client computer, wherein the encrypting instruction encrypts the encryption key with the hardware profile of the client computer.

18. The system of claim 16, wherein the hardware profile of the client computer is stored and linked with a copy of the digital certificate on the server and the determining

instruction retrieves the hardware profile that is linked with the copy of the digital certificate.

19. The system of claim 13, wherein:

the server includes a first hardware profile of the client computer stored and linked with a copy of the digital certificate;

the requesting instruction includes transmitting a second hardware profile of the client computer to the server; and

the determining instruction determines whether the second hardware profile is the same as the first hardware profile.

20. The system of claim 19, wherein the digital certificate includes a public key of a public key infrastructure (PKI) key pair and the client computer software further comprises instructions for:

encrypting the second hardware profile of the client computer with a random session key; and

encrypting the random session key with the public key of the PKI key pair.

21. The system of claim 20, wherein the server includes a copy of the digital certificate including a private key of the PKI key pair and the determining instruction includes decrypting the random session key with the private key of the PKI key pair.

22. The system of claim 13, wherein:

the digital certificate includes a certificate serial number;

the server includes a copy of the digital certificate including the certificate serial number;

the requesting instruction includes transmitting the certificate serial number to the server; and

the determining instruction includes retrieving the copy of the digital certificate using the certificate serial number.

23. The system of claim 13, wherein the receiving instruction receives content from a website server.

24. The system of claim 13, wherein the server is a first server and the receiving instruction receives content from a second server co-located with the first server.

25. A computer-readable medium comprising instructions for digital rights management, by:

receiving content at a client computer, wherein the content is encrypted with an encryption key; and

requesting the encryption key from a digital rights management (DRM) server using a digital certificate, wherein:

the server is remote from the client computer;

the server receives the request; and

the server determines if the digital certificate is valid.

26. The computer-readable medium of claim 25, further comprising instructions for:

receiving the encryption key from the server, wherein the encryption key is encrypted; and

decrypting the encryption key.

27. The computer-readable medium of claim 26, wherein:

the encryption key is encrypted with a hardware profile of the client computer; and

the decrypting instruction decrypts the encryption key with the hardware profile of the client computer.

28. The computer-readable medium of claim 25, wherein:

a first hardware profile of the client computer is stored on the server; and

the requesting instruction includes transmitting a second hardware profile of the client computer to the server, wherein the DRM determines if the digital certificate is valid by comparing the second hardware profile of the client computer to the first hardware profile of the client computer.

29. The computer-readable medium of claim 28, wherein the digital certificate includes a public key of a public key infrastructure (PKI) key pair, further comprising instructions for:

encrypting the second hardware profile of the client computer with a random session key; and

encrypting the random session key with the public key of the PKI key pair.

30. The computer-readable medium of claim 25 wherein:

the digital certificate includes a certificate serial number;

the server includes a copy of the digital certificate including the certificate serial number;

the requesting instruction includes transmitting the certificate serial number to the server; and

the DRM determines if the digital certificate is valid by retrieving the copy of the digital certificate using the certificate serial number.

31. The computer-readable medium of claim 25 wherein the receiving instruction receives content from a website server.

32. The computer-readable medium of claim 25 wherein the server is a first server and the receiving instruction receives content from a second server co-located with the first server.

33. A computer-readable medium comprising instructions for digital rights management, by:

receiving a client computer request, at a digital rights management (DRM) server, for an encryption key using a digital certificate, wherein the client computer receives content that is encrypted with the encryption key; and

determining if the digital certificate is valid.

34. The computer-readable medium of claim 33 further comprising instructions for:

if the digital certificate is valid, transmitting the encryption key to the client computer.

35. The computer-readable medium of claim 34 further comprising instructions for:

encrypting the encryption key, wherein:

the transmitting instruction transmits the encrypted encryption key to the client computer.

36. The computer-readable medium of claim 35 further comprising instructions for:

determining a hardware profile of the client computer, wherein:

the encrypting instructions encrypts the encryption key with the hardware profile of the client computer.

37. The computer-readable medium of claim 36, wherein:

the hardware profile of the client computer is stored and linked with a copy of the digital certificate on the server; and

the determining instruction retrieves the hardware profile that is linked with the copy of the digital certificate.

38. The computer-readable medium of claim 33, wherein

a first hardware profile of the client computer is stored and linked with a copy of the digital certificate on the server;

the request includes a second hardware profile of the client computer; and

the determining instruction determines whether the second hardware profile is the same as the first hardware profile.

39. The computer-readable medium of claim 38, wherein:

the digital certificate includes a public key of a public key infrastructure (PKI) key pair;

the second hardware profile of the client computer is encrypted with a random session key;

the random session key is encrypted with the public key of the PKI key pair;

a copy of the digital certificate including a private key of the PKI key pair is stored on the server; and

the determining instruction includes decrypting the random session key with the private key of the PKI key pair.

40. The computer-readable medium of claim 33 wherein:

the digital certificate includes a certificate serial number;

a copy of the digital certificate that includes the certificate serial number is stored on the server;

the request includes the certificate serial number; and

the determining instruction includes retrieving the copy of the digital certificate using the certificate serial number.